Symantec mise sur le Data Loss Prevention

La Haye (Pays-Bas) – A en croire John Thompson, le CEO de Symantec, la société a choisi de faire de la prévention de fuite de données son cheval de bataille (comme nombre de ses concurrents d'ailleurs, comme Websense).

Depuis la fusion avec la société **Altiris** en janvier dernier, un des leaders des gestionnaires de parcs de PC, mais aussi d'avec Vontu (spécialiste de la prévention de fuites) la firme a pu mettre en place et dévoiler à la presse le **Data Loss Prevention 9.0** (DLP).

Au cœur de la stratégie de l'éditeur pendant ce grand raout de la sécurité « made in Symantec », ce DLP fait partie des 3 annonces majeures annoncées. Cette stratégie d'*Information Risk Management* se traduit par la sortie simultanée de **Brightmail Gateway 8.0**, **Data Loss Prevention 9.0**, et **Enterprise Vault 8.0**.

La suite du DLP de Symantec est donc chargée d'identifier toutes les données d'une société et de les **vider de tout malware le plus rapidement possible.** Une sorte de relais chargé d'identifier les comportements à risque susceptibles d'entraîner des divulgations de données sensibles au sein de l'entreprise.

Ainsi, Data Loss Prevention 9.0 comprend l'agent de gestion de poste client d'Altiris ce qui permet à cette dernière mouture de **surveiller l'utilisation faite du contenu** de postes clients même lorsqu'ils ne sont pas connectés sur le réseau. La suite prend ensuite le rôle de **gendarme de la sécurité** en gérant entre autres les **autorisations de copier/coller de texte**, **d'impression** et de télécopie… en se vantant de tout savoir de ce qu'il se passe dans la base de données.

Pour mettre en place cette nouvelle suite, Symantec part d'un constat : les **fuites ou pertes de données sont le plus souvent le fait d'utilisateurs internes** à la société (en effet !). Et les exemples récents se multiplient, notamment en Grande-Bretagne ou plus récemment en Allemagne (Deutsche Telekom a perdu 17 millions de données de ses clients).

Si la menace est « intérieure » c'est donc qu'il faut savoir quoi et comment sécuriser les informations contenues dans les bases de données. Michael Wolfe, vice-président des solutions DLP s'explique : « *Disposer de compétences pour dénicher un risque n'est pas suffisant, il est nécessaire que le DLP s'adapte aux spécificités de l'entreprise. Il va donc créer un* ***inventaire de ce qu'il faut garder et/ou nettoyer***« .

Symantec continue de jouer les plombiers informatiques, réparateurs de fuites pour un DLP 9.0 disponible dès le début 2009. Encore faut-il être raccord avec les capacités des sociétés à se munir d'une telle suite.